(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
21 February 2002 (21.02.2002)

PCT

(10) International Publication Number
WO 02/14987 A2

(51) International Patent Classification[7]: G06F 1/00

(21) International Application Number: PCT/IB01/01876

(22) International Filing Date: 20 August 2001 (20.08.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/226,128 18 August 2000 (18.08.2000) US
60/259,575 4 January 2001 (04.01.2001) US

(71) Applicant *(for all designated States except US)*: **CAMELOT INFORMATION TECHNOLOGIES LTD.** [IL/IL]; Matam, Advanced Technology Center, 31905 Haifa (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **GADISH, Ofer** [IL/IL]; 8, Shikma Street, 34737 Haifa (IL). **BAHARAV, Yuval** [IL/IL]; 40, Massada Street, 33076 Haifa (IL).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*
— *entirely in electronic form (except for this front page) and available upon request from the International Bureau*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

WO 02/14987 A2

(54) Title: AN ADAPTIVE SYSTEM AND ARCHITECTURE FOR ACCESS CONTROL

(57) Abstract: A network security system and method for protecting network resources from unauthorized access and/or use. An agent device gathers data in regard to all access attempts directed at network resources and supplies this information to an analyzer device that adapts permission levels to correspond with at least the newly supplied information. The permission levels may be used by a guardian agent for the purpose of allowing or denying access to system resources. Such enforcement may further be conducted with respect to each resource access attempt in accordance with a network security policy. A control unit maintains the security policy and generates reports based on data provided from both the agent device and the analyzer device.

AN ADAPTIVE SYSTEM AND ARCHITECTURE FOR ACCESS CONTROL

CROSS REFERENCE TO RELATED APPLICATIONS

[001] This application claims priority to U.S. Provisional Application 60/226,128, filed August 18, 2000 and U.S. Provisional Application 60/259,575, filed January 04, 2001.

FIELD OF THE INVENTION

[002] The present invention relates generally to computer networks and, specifically, to access control with respect to computer networks.

BACKGROUND OF THE INVENTION

[003] Computer networks may consist of vast amounts of information and/or resources, such as files, documents, texts, databases, servers, printers, plotters, etc. (collectively "resources") shared among a large numbers of users. The resources may have a varied degree of sensitivity and may not necessarily be appropriate for use by all the users of the computer network or by users outside the network. This problem is especially pronounced in the business environment where there are global users and where business-to-business (B2B) communications are common.

[004] Thus, in order to protect resources from inappropriate use, each user in the network may be assigned access to only some, rather than all, resources on the network, effectively restricting access by each user to an appropriate subset of those resources. As a result, people with fewer access restrictions may have access to more of the network

resources, while others with more access restrictions may have access to only a limited number of resources. A member of a development group, for example, may be assigned access privileges to resources pertaining to a particular project on which he is working, while at the same time being restricted from access to other management resources. Each user is thus assigned "static" access privileges according to his perceived level or task. Access restrictions may similarly be assigned to the resources themselves. For example, a network printer may be made available to everyone on the network for printing, or it may be restricted to only those individuals who are granted special access.

[005] Typically, access permissions are controlled at the resource level. Thus, each resource would have a corresponding access control list (ACL) generated either during the creation of the resource or at a later date. An ACL usually comprises a list of access entries, each such access entry containing a user's name and his/her associated permissions/restrictions. In some instances, the access entry may comprise a user group (such as accounting, engineering, marketing, etc.) and the associated access permissions/restrictions for that group. The permissions/restrictions typically allow/prevent access to the resource, or allow/deny the performance of various operations by, or on, the resource, such as deleting, reading, writing, or otherwise using the resource.

[006] In certain operating systems (OSs), such as the UNIX® operating system, the ACL has been simplified to allow only three predefined accessibility levels of users: the owner of the resource, the owner's group, and the world, which would include anyone requesting access. For each of these user levels, three basic access permissions may generally be possible: "read", "write", and "execute".

[007] One known method for carrying out access control on a network may be as follows: A person, X, is accepted into an enterprise or organization network, at which point he is associated with a user name and possibly added to one or more user groups. When person X requests access to a certain resource, the access list associated with that resource is consulted and searched for either the user name or the user group(s) associated with person X. Depending on the relevant ACL, access to the particular resource is either permitted or denied. In fact, in conventional systems, the only possible conclusion for a given access request is either to permit or to deny access.

[008] In such a system, the resultant security policy, which may be seen as a collection of all potential access permissions and denials, is distributed throughout the system, with little or no capability for effective management. Some systems include "agents" that monitor access and consult a more global policy, normally centrally located, to each permission grant or denial.

[009] However, known network security methods present several problems. First, since ACLs are typically input manually, the creation of the lists may be time consuming. As the number of users and resources grows, the task becomes more cumbersome and more prone to mistakes such as inappropriate exclusions, accidental inclusions, etc. Moreover, the person who typically sets up the listing, e.g., the system administrator, may not be aware of every user and/or resource on the network. Furthermore, even if the system administrator is aware of the relevant user and resource, he may not know the job requirements and applicability of each, and so he may not be able to determine the appropriate ACL.

[010] Yet another problem with conventional network security systems is the inflexibility of the ACL, which, by the nature of the input process, is predefined. Each

time a change occurs in the system, whether in regard to a user, a resource, or permission therebetween, the ACL must be amended. Furthermore, since the listing is predefined, exceptions are difficult to implement. For example, if a user changes jobs, his group must be manually changed for him to gain access to the shared resources of his new group. If the user is performing a job temporarily, permissions may be needed for only a limited period of time. Certain permissions for him would have to be granted to perform the job and then revoked when no longer needed, requiring that someone remember to revoke the permissions at the later date.

[011] Thus, there exists a need for a more efficient, better defined access control method and for an associated system architecture that provides for flexible, adaptive use.

SUMMARY OF THE INVENTION

[012] An object of the present invention is to provide an access control system and architecture for accessing resources. It is another object of the invention to provide an access control system and architecture for accessing resources such as databases, files, computer peripherals and others.

[013] An embodiment of the present invention, therefore, provides a system adapted for controlling access by one or more users to one or more resources. The system includes at least one agent, which collects data about access attempts concerning the resources, and at least one access analyzer, which receives and processes the collected data. The access analyzer analyzes at least the collected data and generates permission levels based on the analysis.

[014] In accordance with the invention, an "access attempt" is an attempt to gain access to any of the resources on the system, regardless of whether the access is ultimately permitted or not. Thus, an access attempt includes the situations where access

is granted, and also where access is denied. The data collected by the agent can be, for example, behavioral data concerning the users as well as data concerning the resource itself. More specifically, examples of the collected data include; the access distribution of the resource(s), that is, how each resource is allocated to the user(s); the level and frequency of access attempts initiated by particular user(s), etc. The collected data can also include information about activities such as how much CPU time each user utilizes and/or data regarding I/O and application usage.

[015] The permission levels may be access control permission levels, wherein the permission levels are presented as numbers within a given range, and wherein the likelihood that the access attempt is to be permitted is determined based on the value of the permission level. For example, the permission levels may be normalized to a range between 0 and 1 and the access can be permitted/denied depending on whether the permission level is above/below a certain threshold.

[016] The agent may include at least an enforcement means adapted to control access to the resources based on at least the permission levels. A system in accordance with the present invention may further include one or more controllers adapted to provide one or more rules to the agent, wherein the rules may be access control rules.

[017] Additionally, the enforcement means may be adapted to control access to the resources based on at least the permission levels and the rules and, the enforcement means need not necessarily be located within the agent. The enforcement means can be located external to the immediate network and its servers and enforce access to the resources through remote means. In further embodiments of the invention, the system may also include a discovery unit adapted to provide information to the controller,

wherein the information may be data concerning the users and the resources. The discovery unit may include means for automatically gathering the information.

BRIEF DESCRIPTION OF THE DRAWINGS

[018] The object and features of the present invention will become more readily apparent from the following detailed description of the preferred embodiments taken in conjunction with the accompanying drawings in which:

[019] **FIG. 1** is a block diagram illustration of an access architecture, constructed and operative according to an embodiment of the present invention;

[020] **FIG. 2** is a block diagram illustration of an access control system, implemented using the access architecture of FIG. 1, constructed and operative according to an embodiment of the present invention; and

[021] **FIGS. 3A and 3B** are block diagram illustrations of alternative access control systems, implemented using the access architecture of FIG. 1, constructed and operative according to an embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[022] A preferred embodiment of the present invention is discussed in detail below. While specific configurations are discussed, it should be understood that this is done for illustration purposes only. A person skilled in the relevant art will recognize that other components and configurations may be used without departing from the spirit and scope of the invention.

[023] Reference is now made to FIG. 1, which is a block diagram illustrating the operation of the invention and an example of access architecture 10. Architecture 10 illustrates one embodiment of the present invention; other embodiments are also described below.

[024] In order to facilitate the discussion of a preferred embodiment, the following is a list of relevant terms and associated definitions: "Resources" may be services, documents, data, files, databases, or any portion of such services, documents, data, files, databases, as well as peripheral devices or any other type of computer resources. "Access Attempt", as mentioned above, may be an attempt to use or otherwise gain access to a particular resource. "User(s)" may be any person, user group, or other resource wishing to access a resource; persons such as members of a company with which the resource resides, associates of the company (e.g., in a B2B situation), Internet browsers, etc. or programs or other resources. "User groups" may be teams of users with some actual or perceived shared trait, such as shared responsibilities, e.g., an accounting group, shared location, e.g., Haifa group, shared hierarchy in the corporation, e.g., a management group, etc. "Policy" may be a list of rules and "security policy" may be a list of rules that control the access privileges to resources. "Rules" may comprise at least user or user group names and/or associated access permission, denial or other result. "Administrators" may be persons who administer or manage computer systems such as those described herein. A "security policy table" may be a table that lists access options and other rules related to resource security. "Permission levels" refer to the likelihood that accesses to the resource will be required and/or granted. The permission levels may be likelihood estimates, possibly discretized and normalized to a specific range, for example, between 0 and 1. Such a permission level may be specific to the user, his group, time-of-day, location, or other parameters. An "analyzing algorithm" may be an algorithm that, based on gathered data, for example access requests, learns about activities and at least therefrom creates permission levels. "Adaptive permission levels" or "APL" may be permission levels generated periodically by an analyzing algorithm.

An "agent" may be a software utility that collects data about the activities of the computer; a "guardian agent" is a type of agent that is capable of enforcement based on at least security policy rules. A guardian agent may further be capable of enforcement based, in addition, on permission levels.

[025] Illustrated in FIG. 1 is an exemplary system in accordance with the present invention. Three elements comprise an architecture 10: an Agent 100, a Control Unit 110, and an Access Analyzer 120. Agent 100 monitors access attempts 108 directed to particular resources, (not shown), and provides a periodic event audit trail 102 to access analyzer 120, reports alarms 104 to control unit 110 and, if it is a "Guardian Agent", enforces access restrictions 106 to the resource. Event Audit Trail 102, includes information regarding the access attempt(s), including but not limited to such things as whether the access was permitted, time of the access attempt, etc. Access analyzer 120 analyzes event audit trail 102, possibly using a first security policy 122 provided by control unit 110, and responds periodically by sending a list of permission levels 134 to agent 100. Access analyzer 120 also sends statistical information 132 to control unit 110. Based on permission levels 134, received from access analyzer 120 and optionally second security policy 122' received from control unit 110, agent 100, if it is a guardian agent, can provide enforcement 106. Access enforcement 106 includes enforcing the security control of the resources by permitting, alerting, denying, or otherwise controlling access to the resource.

[026] First and second security policy arrows 122 and 122' can represent the same security policy information from control unit 110 to access analyzer 120 and agent 100, respectively, or either the first or second security policy, 122 or 122', can comprise a subset of the other. Independently sending/receiving a security policy allows for the use

of multiple agents 100, access analyzers 120, and control units 110 which all either send or receive united security policy 122, or 122'. Control unit 110 may use the alarms 104 received from agent 100, the statistical information 132 received from Access analyzer 120, and other user inputs (not shown) to create reports 126. Reports 126 provide all, or some, of the input information in a user defined format.

[027] In another embodiment of the present invention (not shown), first security policy 122 can be provided to agent 100 by way of access analyzer 120. In other words, access analyzer 120 receives first security policy 122 from control unit 110 and then sends it along to agent 100. According to this embodiment, it would not be necessary to provide second security policy 122' from Control Unit 110 to Agent 100.

[028] According to the architecture 10, described above, a system in accordance with the present invention may be used for various operations, including analysis, intrusion detection, website user profiling, database access, or any other resource access application, such as access control.

[029] FIG. 2, to which reference is now made, provides a relatively detailed illustration of an exemplary configuration of architecture 10, herein referred to as an access control architecture, or access system 20, which is constructed and operative in accordance with an embodiment of the present invention. Access system 20 comprises one or more agents 100, one or more access analyzers 120, one or more central control servers 110, an optional security policy (not shown) originating in control server 110, and optionally one or more auto discovery units 22. Access system 20 resides, for example, in a university, business, or any other organization, that has one or more servers 18, 18' and 18" which may communicate with other devices through either non-secure or secure channels (e.g., encrypted channels). Servers 18, 18' and 18'' include any computer

resources that serve as gateways to other computer resources or services. Exemplary servers shown in FIG. 2 are databases 18', file servers 18", and personal computers 18, but other, similar machines, such as printer servers (not shown), could also be connected to system 20 in accordance with the present invention.

[030] In accordance with the present invention, system 20 can utilize one or more adaptive algorithms. For example, system 20 may be dedicated to the adaptive access control of resources on a network, as depicted in architecture 10 (FIG. 1). Optionally, for secure embodiments of the present invention, system 20 may also comprise a key authority (not shown), which can reside on control server 110 or on another appropriate platform. In a secure embodiment of the present invention, all communications to/from each device can be encrypted in accordance with conventional encryption tehniques. For example, each of the devices shown in FIG. 1, for example, Agent 100, Access Analyzer 120 and Control Unit 110, can be equipped with both encryption and decryption tools in order to encrypt the information it sends, and decrypt the information it receives.

Agent

[031] Agents 100, which may also be Guardian Agents as described above, reside on servers 18, 18' or 18" and monitor access attempts that occur on servers 18, 18' or 18" and gather data related to those access attempts, data such as the name of the user attempting access, the machine from which access is attempted, the time of day of the access attempt, the resource to which access is attempted, the type of access attempted, etc. The gathered data may then be sent as event audit trail 102 (FIG. 1) to access analyzer 120 to be used as input for an analyzing algorithm run by access analyzer 120. The analyzing algorithm can use at least the gathered data to generate permission levels 134 (FIG. 1).

[032] In further embodiments, based on at least the permission levels 134, guardian agents 100 can protect the resources stored on servers 18, 18' or 18" by enforcing the permission levels 134. Enforcement may be performed by guardian agent 100 or by an enforcement unit (not shown) provided either within guardian agent 100 or as a separate unit.

[033] In yet another embodiment of this invention, event audit trail 102 is used by access analyzer 120 to generate the underlying system permissions, e.g., ACLs, that are used to update the system ACLs. In this embodiment, agent 100 may not necessarily be a guardian agent. In another embodiment of this invention, the consulting facilities of a computer system may be used. In such a case as a response to an access attempt 108 the system will respond with a query to the consulting facilities. The consulting facilities, based on permission levels provided by access analyzer 120 may respond with the required response relative to access attempt 108. In yet another embodiment of this invention, agent 100 may be implemented as a "proxy", i.e., a unit through which all the network traffic flows and which may not necessarily be part of the system it is protecting, and access attempts 108 will be handled from the "proxy" unit.

[034] Also, agents 100 can reside on control server 110 or any other appropriate platform. That is, it is not necessary for Agents 100 and Control Units 110 to be separate machines, their functionalities can be combined into a single machine.

[035] In other embodiments, based on at least the permission levels 134 and the security policy 122, 122', guardian agents 100 may protect the resources stored on servers 18, 18' or 18" by executing and enforcing access permissions and restrictions, and possibly notifications to other system resources, based on both the permission levels 134 and security policies 122, 122' to control access to the resources. As mentioned

above, enforcement may be executed by guardian agent 100 or by an enforcement unit (not shown) within guardian agent 100, or as a separate unit.

Access Analyzer

[036] Access Analyzer 120 may be in communication with one or more agents 100 and each access analyzer 120 can support and control each of these agents 100, depending on the load of each agent 100 and the strength of access analyzer 120. Access analyzer 120 may further receive event audit trail 102 by a push, i.e., where the sender initiates the transfer, or pull, where the receiver initiates the transfer, method to transfer the event audit trail data from each agent 100, applying the data to an analyzing algorithm. For example, the transfer of event audit trail 102 may take place on a cyclic basis (e.g., once a day) and the analyzing algorithm may then be executed after the new event audit trail 102 data has been received.

[037] Access analyzer 120 can utilize any learning algorithm adapted for access control, an example of which is described in the co-pending U.S. Patent Application, filed on the same date herewith, entitled "Permission Level Generation Based on Adaptive Learning", and which is assigned to the same common assignee as the present application, and is incorporated herein by reference in its entirety for all it discloses.

[038] Access analyzer 120, based on security policy 122 and event audit trail 102, is operable to estimate the probability of an access attempt to a system resource occurring and, subsequently, define the most up-to-date permission levels 134. Permission levels 134, which are an output of the analyzing algorithm utilized within Access Analyzer 120, may be transmitted to agent 100, which may receive and/or transmit data to one or more access analyzers 120.

Central Control Unit

[039] Control unit 110 may comprise means for interacting with access analyzers 120 and agents 100, and can manage activities within the system architecture 10 (FIG. 1) and system 20 (FIG. 2) having a single security policy, i.e., a combination of security policies 122, 122'. In other embodiments of the present invention, one or more control servers 110 may handle a single security policy. Control server 110 may control the system configuration, security policy, and response to reported events. When access attempts 108 occur, they may be reported to control unit 110, and, based on the nature of the attempt, control unit 110 may notify the appropriate person(s) or program(s) by e-mail or other form of communication. Control unit 110 may include a database, a report generation engine, and a scheduler.

[040] In a further embodiment in accordance with system 20, agents 100 may monitor access attempts 108 that occur on servers 18, 18' and 18" and gather data related to those attempts. The access attemtps and data that are monitored may relate to user or resource activities, or to any other operations that may occur on servers 18, 18' or 18". The access attempts 108 that are monitored may include resource retrieval and/or usage of, for example, documents, files, databases, computer peripherals, etc., resource accesses, logins, internal communication problems, access times and types, etc. Event audit trail 102 may include the number of times a resource is accessed, the users that access a specific resource, access time, type of access, any type of statistical data related to the access attempt, etc.

[041] Event audit trail 102 may be used as an input for the analyzing algorithm run by access analyzer 120 as mentioned above. In some embodiments of the invention, the analyzing algorithm uses at least event audit trail 102 to generate permission levels 134

for respective accesses to resources. Permission levels 134 may be specific to each type of access, they may be time dependent, and/or they may correspond to each user and each resource.

[042] Agent 100 may receive permission levels 134 from access analyzer 120 and may receive security policy 122', in the form of a table, or some other format, from control unit 110. In some embodiments of the invention, rules related to the security policy may be defined in control unit 110 and enforced by a guardian agent type of agent 100.

[043] Based on at least permission levels 134 and second security policy 122' guardian agent 100 may execute and enforce the overall access requirements of the resource, thereby protecting the resources stored on servers 18, 18' or 18" from unauthorized access or use. Security policy rules may include a first threshold below or above which an alarm will be generated to notify the control unit 110 of an access attempt to a resource. Security policy rules may also include a second threshold below or above which access attempts to a resource will be denied. An example of a security policy including the security policy rules just described is in the co-pending U.S. Patent Application, filed on the same date herewith, entitled "A Method and Apparatus for a Security Policy", and assigned to common assignee of the present invention, and which is incorporated in its entirety herein by reference for all that is disclosed.

[044] Enforcement may comprise two different operations. For example, enforcement can include; 1) allowing operations that are permitted by both the security policy and the permission levels, if both exist, or; 2) blocking operations that are not permitted or are considered suspicious beyond a second threshold level mentioned above. The second operation may further include the generation of a different alarm if an operation is considered suspicious as is beyond a first level threshold.

[045] Enforcement may be performed by guardian agent 100 or by an enforcement unit (not shown) within guardian agent 100. Alternatively, agents 100 may reside on control unit 110 or any other appropriate platform having access to system resources.

[046] The security policy rules and permission levels 134 may correspond to a user, a group of users, a resource, a group of resources or a combination of user(s) and resources(s). The security policy rules may also be applied on an access type and/or time basis, and/or may be applied on the basis of access parameter availability, such as location. User groups may be created by applying an algorithm, observing formal or informal hierarchy, or other method known in the art.

[047] Security policy rules may correspond to a resource, a user, or a <resource, user> pair, possibly in combination with a particular time, and access type as mentioned above. Agent 100 may determine which rules apply to each resource, each user, and each <resource, user> pair at each time. Enforcement determinations can be made on the basis of at least the rules and/or on other factors, such as location. Conflicts between rules that are defined for the same <resource, user> pair may be resolved in the security policy rules or flagged by the system, which can determine how to handle conflicts. The system may, for example, always follow the first security policy rule matching the access attempt. In another embodiment, the system may, for example, always follow the stricter of conflicting security policy rules.

[048] In further embodiments of the invention, agent 100 may protect specific resources by applying adaptive access control only to specific resources of the existing security system. In such embodiments, agent 100 does not replace or use any of the existing security subsystem. Instead, agent 100 may, in addition to following the specific resource rules, continue to enforce the system's existing rules and thus, may not

permit anything that is blocked by the existing security subsystem. For example, if the operating system (OS) already permits/denies access to certain resources based on its own independent rules, the adaptive access control system of the present invention will not override the OS's rules and allow access to users that would otherwise not be permitted access.

[049] By being an extension of the existing system, agent 100 can further provide a uniform interface between the various systems since the rules of other existing systems are incorporated without the need to interface with those systems directly. Interfacing to other systems in this manner satisfies the definition of unified and universal security policy rules.

[050] There may be an agent 100 for each platform or application, and agent 100 may be implemented as an extension of the operating system (OS), a database, a Web-server, or an application.

[051] Discovery units 22 may comprise a tool used by control unit 110 to obtain information concerning users and resources on servers 18, 18' or 18". Discovery units 22 can receive instructions from control unit 110, when appropriate. For example, discovery unit 22 can collect information regarding which users are defined on servers 18, 18' or 18" and which resources are defined, or any other information that may be useful to control unit 110. As a further example, in some embodiments of the invention, discovery units 22 can report which users are logged-on the respective system. Discovery units 22 can gather information automatically or in response to a request from control unit 110 and Discovery units 22 may be a part of agent 100 or they can be a stand-alone units.

[052] Access analyzer 120 can be in communication with agent 100 and receive event audit trail 102. Event audit trail 102 can be used as an input to access analyzer 120 and used in accordance with an adaptive access control analyzing algorithm, in which at least some of the output of the analyzing algorithm, for example permission levels 134, may be used as part of the enforcement 106.

[053] In order for access analyzer 120 to generate access control permission levels 134, the analyzing algorithm can use "Knowledge" pertaining to user activity. Knowledge is derived from the data gathered by agents 100. The data used in gaining "Knowledge" about user activity can be transferred from agents 100 to access analyzers 120 as frequently, or infrequently, as necessary, such as daily, bi-weekly, etc. Updated data can be matched with past (known) user behavior patterns, and the behavior patterns can be updated by access analyzer 120. By consulting the user behavior patterns, it is possible to analyze and determine what each user does, what the relationships between users are, and which resources are likely to be used by various users (or user groups) in the future. As mentioned above, an exemplary analyzing algorithm is described in the co-pending U.S. Patent Application, filed on the same date herewith, entitled "Permission Level Generation Based on Adaptive Learning".

[054] Furthermore, access analyzer 120 can generate permission levels, possibly by calculating the likelihood that a particular access attempt should be permissible. The permission levels are numbers in a given range, wherein the higher the number the more likely the access attempt is to be permitted. The permission levels may be normalized to a range between 0 and 1, or any other appropriate range or scale.

[055] In some embodiments of the invention, access control determinations can be made in run-time by agent 100. In such an instance, access analyzer 120 provides the permission levels 134 to agent 100 in advance or in generally real-time.

[056] Providing organizational structure of users information of the system to the analyzing algorithm is optional. In other words, the analyzing algorithm can operate using only the data gathered by agent 100. Nevertheless, the analyzing algorithm can accept additional data, such as organizational structure information, if provided. Additional data, such as the OS permissions, or feedback from users, may improve the quality of the results, shorten the run time of the analyzing algorithm, or reduce the numbers of runs of the analyzing algorithm until convergence, or a good result, is achieved. Conversely, false input can reduce quality or increase run-time. However, given that the algorithm can resolve inaccuracies by "learning", the false input may not cause completely incorrect determinations, and effects of such will be practically eliminated over time.

[057] Control unit 110 can request that agent 100 gather information upon demand. Control unit 110 can also act as a cryptographic key manager, serving as a certificate authority, and can, further maintain a list of system administrators and their associated privileges.

[058] When access attempts 108 occur, they may be reported to control unit 110, and, based on the nature of the event, control unit 110 may notify the appropriate person(s) and/or log the events outlined in the reports for future reference. Control unit 110 can be operable to prepare and generate reports, schedule activities for execution, save the reports in an archive, and/or optionally distribute the reports by email, links, or other means of communication, to a recipient list, and/or link to them.

[059] In accordance with an embodiment of the present invention, the following is an exemplary access control scenario: Agent 100 monitors a request for access to a certain resource. Agent 100 either has or receives security policy 122' (including rules) from control unit 110. Agent 100 also either has or receives permission levels 134 from access analyzer 120. Based on permission levels 134 and security policy 122', agent 100, if it is a guardian agent, provides enforcement 106. Enforcement 106 comprise of blocking access, permitting access, reporting the access attempt, etc.

[060] Access analyzer 120 receives from agent 100 data about the access attempt and executes the analyzing algorithm. The output of the analyzing algorithm may be permission levels 134, which are transferred periodically to agent 100. The activities of agent 100 and access analyzer 120 may be time-independent with respect to each other. For example, while agent 100 operates on each and every access attempt 108, access analyzer 120 may operate periodically, based on sufficient information collected from event audit trail 102, or at the conclusion of a predefined period of time.

[061] Control unit 110 can be notified of the access attempt and any subsequent confirmation of enforcement and can generate a report based on the data for on-line review or for distribution.

[062] An important feature of the present invention is that each of the parts – agent 100, access analyzer 120, and control unit 110 – can operate independently. That is, agent 100 can continue operating even if its connection to access analyzer 120 is not operative. For example, Agent 100 can continue gathering event audit trail data and use its latest stored version of permission levels 134 even if no updated permission levels are being provided. Access analyzer 120 can perform the analyzing algorithm using the latest event audit trail data it has received, whether or not agent 100 is currently

communicating with access analyzer 120. Likewise, access analyzer 120 can perform the analyzing algorithm using the latest security policy 122 it has received, whether or not control unit 110 is currently communicating. Control unit 110 can be used at any time to set overall security policy 122, 122', which is transmitted to access analyzer 120 and agent 100, when possible. Finally, statistical information 132 and alarms 104 can be received by control unit 110 when any disrupted connections are eventually restored, and reports 126 can be generated independently, periodically or upon request.

[063] System 20 is further operable on alternative architectures, such as those illustrated in FIGS. 3A and 3B, which show architectures 30 and 40, respectively, to which reference is now made. Architecture 30 is a simple configuration that may be applicable for small businesses. As shown in FIG. 3A, architecture 30 can comprise control unit 110 and file server 18, with the components of agent 100 and access analyzer 120 both residing on server 18. Architecture 30 can provide the compactness and flexibility needed for small computing environments.

[064] Alternatively, architecture 40, shown in FIG. 3B may be applicable for application service providers (ASPs), and may operate on a local or non-local system, such as the Internet or web, and may operate on a direct line, without intermediate providers. Architecture 40 may comprise at least one file server 18, one or more optional firewalls 28, and an application server 32. As noted in FIG. 3B, in order to adapt to the appropriate architecture and/or system, the components of agent 100 may be operable from file server 18. Access analyzer 120 and control unit 110 may reside on application server 32. Application server 32 may be connected to file server 18 through firewalls 28 and over the Internet. This will allow for a remote implementation of the security system by an application provider.

[065] It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described herein above. Rather the scope of the invention is defined by the claims that follow.

WHAT IS CLAIMED IS:

1. A computer network with a security system, the security system comprising:

at least one agent operable to identify an access attempt directed to a resource on the network and further operable to respond to said access attempt in accordance with at least permission levels; and

at least one access analyzer operable to analyze an event audit trail and provide said permission levels to said agent.

2. The computer network of claim 1, further comprising at least one control unit operably connected to said agent and said access analyzer.

3. The computer network of claim 2, wherein said control unit comprises at least a security policy.

4. The computer network of claim 3, wherein said guardian agent implements a unified security policy which is a unification of the said systems original security policy and an security policy operable with at least said permission levels.

5. The computer network of claim 4, wherein said unified security policy implements the most restrictive rules.

6. The computer network of claim 4, wherein said unified security policy implements the most permissive rules.

7. The computer network of claim 3, wherein said security policy comprises at least one security rule.

8. The computer network of claim 7, wherein said security rule defines at least one response to said access attempt.

9. The computer network of claim 8, wherein said response comprises at least allowing an access.

10. The computer network of claim 8, wherein said response comprises at least denying an access.

11. The computer network of claim 8, wherein said response comprises at least notification of an access.

12. The computer network of claim 8, wherein said response is adaptive in accordance with at least said permission levels.

13. The computer network of claim 12, wherein said adaptive response is further determined in accordance with at least one activation threshold.

14. The computer network of claim 13, wherein said response comprises at least allowing an access, determined at least in accordance with a first activation threshold.

15. The computer network of claim 13, wherein said response comprises at least denying an access, determined at least in accordance with a first activation threshold.

16. The computer network of claim 13, wherein said response comprises at least notification of an access, determined at least in accordance with a second activation threshold.

17. The computer network of claim 2, further comprising a discovery unit operable to provide information to said control unit.

18. The computer network of claim 17, wherein said information includes data relative to at least a user of said network.

19. The computer network of claim 17, wherein said information includes data relative to at least a resource accessible through said network.

20. The computer network of claim 17, wherein gathering of said information is automatic.

21. The computer network of claim 2, wherein said access analyzer provides said agent with only deny or permit status for each access attempt.

22. The computer network of claim 1, further comprising at least one control unit operably connected to said access analyzer.

23. The computer network of claim 22, wherein said control unit comprises at least a security policy.

24. The computer network of claim 23, wherein said guardian agent implements a unified security policy which is a unification of the said systems original security policy and an security policy operable with at least said permission levels.

25. The computer network of claim 24, wherein said unified security policy implements the most restrictive rules.

26. The computer network of claim 24, wherein said unified security policy implements the most permissive rules.

27. The computer network of claim 23, wherein said security policy comprises at least one security rule.

28. The computer network of claim 27, wherein said security rule defines at least one response to said access attempt.

29. The computer network of claim 28, wherein said response comprises at least allowing an access.

30. The computer network of claim 28, wherein said response comprises at least denying an access.

31. The computer network of claim 28, wherein said response comprises at least notification of an access.

32. The computer network of claim 28, wherein said response is adaptive in accordance with at least said permission levels.

33. The computer network of claim 32, wherein said adaptive response is further determined in accordance with at least one activation threshold.

34. The computer network of claim 33, wherein said response comprises at least allowing an access, determined at least in accordance with a first activation threshold.

35. The computer network of claim 33, wherein said response comprises at least denying an access, determined at least in accordance with a first activation threshold.

36. The computer network of claim 33, wherein said response comprises at least notification of an access, determined at least in accordance with a second activation threshold.

37. The computer network of claim 22, further comprising a discovery unit operable to provide information to said control unit.

38. The computer network of claim 37, wherein said information includes data relative to at least a user of said network.

39. The computer network of claim 37, wherein said information includes data relative to at least a resource accessible through said network.

40. The computer network of claim 37, wherein gathering of said information is automatic.

41. The computer network of claim 22, wherein said access analyzer provides said agent with only deny or permit status for each access attempt.

42. The computer network of claim 1, wherein said agent responds to said access attempt in accordance with a result of comparing at least one permission level to at least one threshold.

43. The computer network of claim 42, wherein said agent permits access to said resource if the permission level exceeds a first threshold.

44. The computer network of claim 42, wherein said agent denies access to said resource if the permission level does not exceed a first threshold.

45. The computer network of claim 42, wherein said agent sends a notification of said access attempt to said control unit if the permission level is below a second threshold.

46. The computer network of claim 1, wherein said access attempt comprises at least one of: a user, a resource, a location, an access type, a time.

47. The computer network of claim 46, wherein said user may be one or more users.

48. The computer network of claim 46, wherein said resource may be one or more resources.

49. The computer network of claim 46, wherein said location may be one or more locations.

50. The computer network of claim 46, wherein said access type comprises at least one of the following; read, write, modify, execute, delete, rename, take ownership of, change permissions of, or create said resource.

51. The computer network of claim 1, wherein said access attempt comprises at least a time scope.

52. The computer network of claim 1, wherein said event audit trail is derived from at least one access attempt.

53. The computer network of claim 52, wherein said event audit trail is provided to said access analyzer on a periodic basis.

54. The computer network of claim 52, wherein said event audit trail is periodically solicited by said access analyzer.

55. The computer network of claim 52, wherein said access attempt is ignored by said agent with respect to at least one access attempt.

56. The computer network of claim 1, wherein said permission levels are derived from at least likelihood estimates that a future access attempt should be permitted.

57. The computer network of claim 1, wherein said agent comprises at least one enforcement means for controlling access to said resources based on at least said permission levels.

58. The computer network of claim 1, wherein said permission levels are generated periodically based on a currently available event audit trail.

59. The computer network of claim 1, wherein said agent and said access analyzer reside on a single computer.

60. The computer network of claim 2, wherein said agent and said control unit reside on a single computer.

61. The computer network of claim 2, wherein said access analyzer and said control unit reside on a single computer.

62. The computer network of claim 2, wherein said agent, said access analyzer and said control unit reside on a single computer.

63. The computer network of claim 1, wherein said permission levels generated by said access analyzer are used for the purpose of updating at least an access control list of at least a system resource.

64. The computer network of claim 1, wherein said access analyzer provides permission level information to at least a system consulting unit.

65. The computer network of claim 64, wherein in response to said access attempt a query is sent to said system consulting unit.

66. The computer network of claim 65, wherein in response to said query asid system consulting unit provides a response corresponding at least to said permission levels.

67. The computer network of claim 1, wherein said agent is implemented as a proxy server.

68. A system comprising a computer network with a distributed security system, the system further comprising:

at least one agent connected to the Internet, said agent being operable to identify an access attempt directed to a resource on the computer network and further operable to respond to said access attempt in accordance with at least permission levels;

at least one access analyzer connected to the Internet, said access analyzer being operable to analyze an event audit trail and provide said permission levels to said agent; and

a communication device operable to provide communication between said agent and said access analyzer.

69. The system of claim 68, wherein the agent is connected to the Internet through a firewall.

70. The system of claim 68, wherein the access analyzer is connected to the Internet through a firewall.

71. The system of claim 68, further comprising at least one control unit operably connected to the Internet.

72. The system of claim 71, wherein the control unit is connected to the Internet through a firewall.

73. The system of claim 71, wherein said control unit and said access analyzer are implemented on the same computer.

74. The system of claim 71, wherein said control unit and said access analyzer are implemented on the same intranet.

75. The system of claim 71, wherein said control unit and said agent are implemented on the same computer.

76. The system of claim 71, wherein said control unit and said agent are implemented on the same intranet.

77. The system of claim 71, wherein said guardian agent implements a unified security policy which is a unification of the said systems original security policy and an security policy operable with at least said permission levels.

78. The system of claim 77, wherein said unified security policy implements the most restrictive rules.

79. The system of claim 77, wherein said unified security policy implements the most permissive rules.

80. The system of claim 77, wherein said security policy comprises at least one security rule.

81. The system of claim 80, wherein said security rule defines at least one response to said access attempt.

82. The system of claim 81, wherein said response comprises at least allowing an access permission.

83. The system of claim 51, wherein said response comprises at least denying an access.

84. The system of claim 81, wherein said response comprises at least notification of an access.

85. The system of claim 81, wherein said response is adaptive in accordance with at least said permission levels.

86. The system of claim 85, wherein said adaptive response is further determined in accordance with at least one activation threshold.

87. The system of claim 86, wherein said response comprises at least allowing an access, determined at least in accordance with a first activation threshold.

88. The system of claim 86, wherein said response comprises at least denying an access, determined at least in accordance with a first activation threshold.

89. The system of claim 86, wherein said response comprises at least notification of an access, determined at least in accordance with a second activation threshold.

90. The system of claim 69, further comprising a discovery unit operable to provide information to said control unit.

91. The computer network of claim 90, wherein said information includes data relative to at least a user of said network.

92. The computer network of claim 90, wherein said information includes data relative to at least a resource accessible through said network.

93. The computer network of claim 90, wherein gathering of said information is automatic.

94. The system of claim 68, wherein said agent responds to said access attempt in accordance with a result of comparing at least one permission level to at least one constant threshold.

95. The system of claim 94, wherein said agent permits access to said resource if the permission level exceeds a first threshold.

96. The system of claim 94, wherein said agent denies access to said resource if the permission level does not exceed a first threshold.

97. The system of claim 94, wherein said agent sends a notification of said access attempt to said control unit if the permission level is below a second threshold.

98. The system of claim 68, wherein said access attempt comprises at least one of: a user, a resource, a location, an access type, a time.

99. The system of claim 68, wherein said user may be one or more users.

100. The system of claim 68, wherein said resource may be one or more resources.

101. The system of claim 68, wherein said location may be one or more locations.

102. The system of claim 68, wherein said access type comprises at least one of the following; read, write, modify, execute, delete, rename, take ownership of, change permissions of, or create, said resource.

103. The system of claim 68, wherein said access attempt comprises at least a time scope.

104. The system of claim 68, wherein said event audit trail is derived from at least one access attempt.

105. The system of claim 104, wherein said event audit trail is provided to said access analyzer on a periodic basis.

106. The system of claim 104, wherein said event audit trail is periodically solicited by said access analyzer.

107. The system of claim 104, wherein said access attempt is ignored by said agent with respect to at least one access attempt.

108. The system of claim 68, wherein said permission levels are derived from at least likelihood estimates that a future access attempt should be permitted.

109. The system of claim 68, wherein said agent comprises at least one enforcement means for controlling access to said resources based on at least said permission levels.

110. The system of claim 68, wherein said permission levels are generated periodically based on a currently available event audit trail.

111. The system of claim 68, wherein said agent and said access analyzer reside on a single computer.

112. The system of claim 71, wherein said agent and said control unit reside on a single computer.

113. The system of claim 71, wherein said access analyzer and said control unit reside on a single computer.

114. The system of claim 71, wherein said agent, said access analyzer and said control unit reside on a single computer.

115. The system of claim 68, wherein said permission levels generated by said access analyzer are used for the purpose of updating at least an access control list of at least a system resource.

116. The system of claim 68, wherein said access analyzer provides permission level information to at least a system consulting unit.

117. The system of claim 116, wherein in response to said access attempt a query is sent to said system consulting unit.

118. The system of claim 117, wherein in response to said query asid system consulting unit provides a response corresponding at least to said permission levels.

119. The system of claim 68, wherein said agent is implemented as a proxy server.

120. A method for controlling access to resources available through the system, said method comprising:

establishing a first threshold value;

gathering an event audit trail comprising data corresponding to at least one access attempt;

periodically analyzing said event audit trail;

generating a permission level for accessing system resources from at least said event audit trail; and

controlling access to said resources based on said generated permission level.

121. A method as claimed in claim 120, wherein said generated permission level comprises adaptive permission levels generated by periodically automatically modifying said event audit trail to account for the most recent access attempt or access attempts.

122. The method of claim 120, wherein if said permission level exceeds said first threshold value, access to said resource is permitted.

123. The method of claim 120, wherein if said permission level does not exceed said first threshold value access to said resource is denied.

124. The method of claim 120, further comprising:

establishing a second threshold value; and

generating a notification if said permission level is below said second threshold value.

125. The method of claim 120, wherein said permission levels are derived from at least at least likelihood estimates that a future access attempt should be permitted.

126. The method of claim 125, wherein said likelihood calculations comprise a probability that a future access attempt should be permitted.

127. The method of claim 120, further comprising:

discovering information about users and said resources.

128. The method of claim 127, wherein said discovering occurs automatically.

129. A method for employing adaptive permissions for accessing system resources comprising of the steps of:

establishing a system security policy said security policy containing at least one adaptive security rule;

gathering an event audit trail of at least one access attempt;

periodically analyzing said event audit trail;

generating permission levels for accessing system resources from at least said event audit trail and said security policy; and

controlling access to said resources based on said generated permission levels.

130. The method of claim 129, wherein the security policy is formatted as a security policy table.

131. The method of claim 129, wherein said adaptive security rule comprises at least one threshold.

132. The method of claim 131, wherein if said permission level exceeds said first threshold value access to said resource is permitted.

133. The method of claim 131, wherein if said permission level does not exceed said first threshold value access to said resource is denied.

134. The method of claim 131, wherein if said permission level is below said second threshold value a notification is generated.

135. The method of claim 129, wherein said permission levels are derived from at least the likelihood estimates that a future access attempt should be permitted.

136. The method of claim 129, further comprising the step of discovering information about users and said resources.

137. The method of claim 136, wherein said step of discovering is automatic.

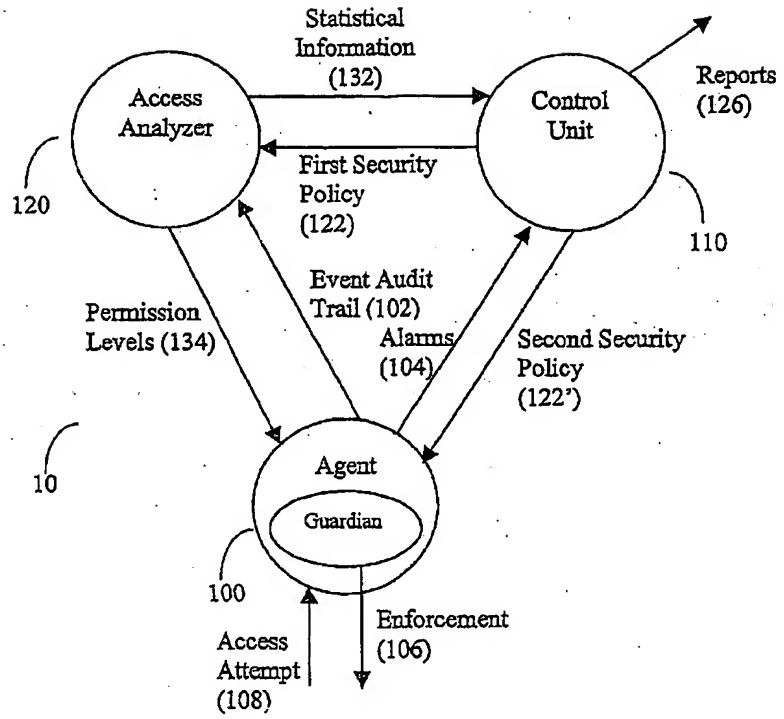
Statistical Information (132)
Access Analyzer
Control Unit
Reports (126)
120
First Security Policy (122)
110
Event Audit Trail (102)
Permission Levels (134)
Alarms (104)
Second Security Policy (122')
10
Agent
Guardian
100
Enforcement (106)
Access Attempt (108)

FIG.1

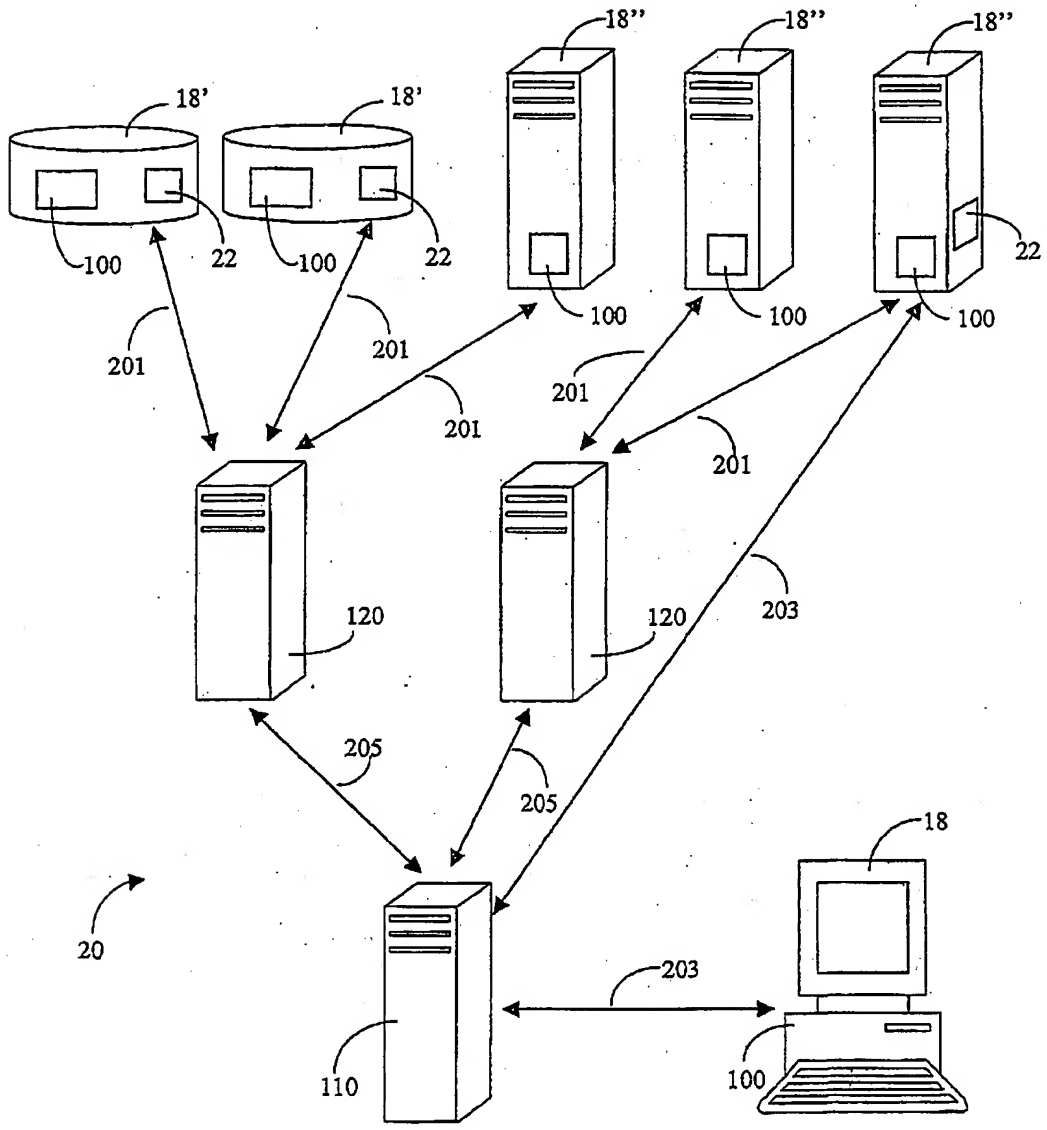
18''
18''
18''
18'
18'
100
22
100
22
100
100
100
22
201
201
201
201
201
201
120
120
203
205
205
18
20
203
110
100

FIG. 2

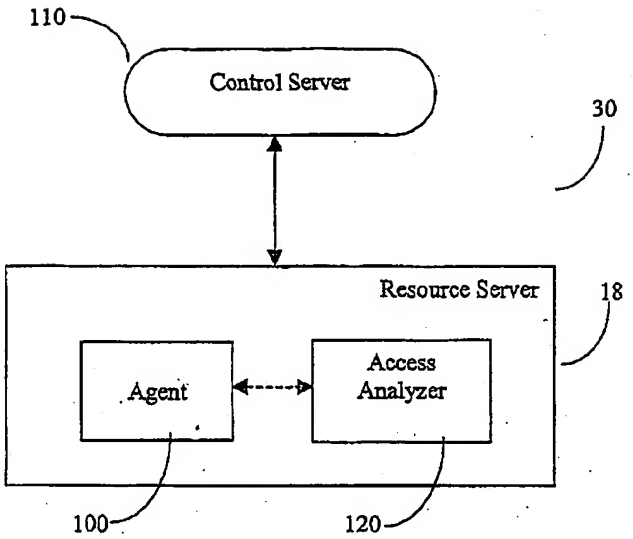
110
Control Server
30
Resource Server
18
Agent
Access Analyzer
100
120

FIG. 3A

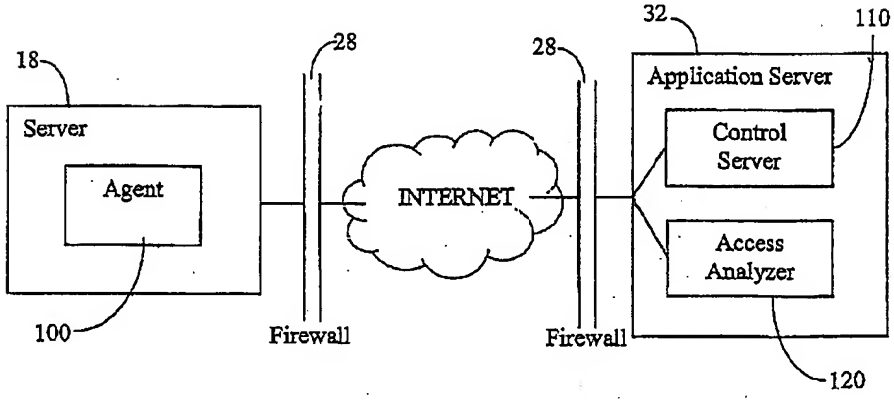
18
Server
Agent
100
28
Firewall
INTERNET
28
Firewall
32
110
Application Server
Control Server
Access Analyzer
120

FIG. 3B